IN THE CLAIMS

Please amend the claims as follows:

1. (Amended) A cryptographic device, comprising:

means for performing one or more cryptographic operations; and

a data storage device or devices for storing access permission data representing the availability of one or more cryptographic characteristics in accordance with which one or more of the cryptographic operations are performed, wherein all of the access permission data of the cryptographic device is stored in the data storage device or devices such that once a value or values of the access permission data are stored in the data storage device or devices, the value or values of the access permission data cannot be changed.

4. (Amended) A computer readable storage medium encoded with instructions and/or data, comprising:

instructions and/or data for performing one or more cryptographic operations; and

access permission data stored in accordance with a predefined data structure, the access permission data representing an availability of one or more cryptographic characteristics in accordance with which one or more cryptographic operations are performed by a cryptographic device, wherein all of the access permission data is stored in the storage medium such that once a value or values of

the access permission data are stored in the storage medium, the value or values of the access permission data cannot be changed.

6. (Amended) A cryptographic device, comprising:

a processor for executing instructions and/or accessing data to perform one or more cryptographic operations that each necessitate the performance of one or more sub-operations;

one or more data storage devices for storing a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation, and a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and

means for allowing access to the first set of instructions and/or data from a device external to the cryptographic device.

14. (Amended) A computer readable storage medium encoded with one or more computer programs for enabling performance of cryptographic operations, comprising:

a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation;

a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and

a third set of instructions and/or data for allowing access to the first set of instructions and/or data from a device external to a cryptographic device of which the computer readable storage medium is part.

15. (Amended) A computer readable storage medium as in Claim 14, wherein the one or more sub-operations comprise one or more mathematical primitive operations.

17. (Amended) A computer readable storage medium as in Claim 14, wherein the cryptographic operations include one or more of the following: RSA encrypt, RSA decrypt, DSA sign, DSA verify, Diffie-Hellman and elliptic curve.

Please enter the following new claims:

18. (New) A computer readable storage medium as in Claim 4, further comprising a programmable read-only memory for storing the access permission data.

19. (New) A cryptographic device as in Claim 6, further comprising means for controlling access to the first and second sets of instructions and/or data, wherein:

the means for controlling access to the first and second set of instructions and/or data comprises the means for allowing access to the first set of instructions and/or data; and

the means for allowing access to the first set of instructions and/or data does not enable access to the second set of instructions and/or data.

20. (New) A computer readable storage medium as in Claim 14, further comprising a fourth set of instructions and/or data for controlling access to the first and second sets of instructions and/or data, wherein:

the fourth set of instructions and/or data comprises the third set of instructions and/or data; and

the third set of instructions and/or data does not enable access to the second set of instructions and/or data.